I. Galois Theory

Several of the concepts from [**Algebra I**], like normal subgroups and finite fields, go back to Galois around 1830. His most important paper, the "Mémoire sur les conditions de résolubilitié des équations par radicaux", was written when he was 19. Around the same time, he was expelled from university for his anti-monarchist political activities. A few months later he received the rejection of this paper in prison; and a year later, not long after being released, was killed in a duel. He was a passionate person who lived in a turbulent time and lost his father to suicide when he needed him most.

In his article, Galois considered groups of permutations of the roots of a polynomial $f(x)$ over $\mathbb{Q}$, which preserve all algebraic relations among these roots. We now think of these "Galois groups" in terms of automorphisms of the field extension generated by these roots. Galois discovered a correspondence between intermediate fields in the extension and subgroups of the Galois group. This leads to the main result of the theory, that the original equation $f(x) = 0$ may be solved by radicals if and only if its Galois group is *solvable* (a term we'll define in due course).

From this, one immediately recovers the insolubility by radicals of a general quintic equation, which had already been proved by Ruffini and Abel; but one also gets criteria for when (and how) a non-general polynomial of degree ≥ 5 *can* be solved. There are many other concrete, attractive applications we will meet along the way, such as the impossibility of trisecting an angle, duplicating a cube, or constructing a regular 7-gon with straightedge and compass; and we shall also be able to tie off some loose ends from our brief study of algebraic number rings [**Algebra I**, §III.L].

I.A. Field extensions

Some of what follows will be review from [**Algebra I**]: in particular, the case of an algebraic extension will look familiar.

Let K be a field.

I.A.1. DEFINITION. An **extension** of K is a pair (ι, L) consisting of a field L and a field homomorphism[1] $\iota\colon K \hookrightarrow L$. (We will often suppress the "ι", especially when we are considering K as a subfield of L, viz. $K = \iota(K)$.)

I.A.2. EXAMPLE. So why would we care about the specific map? The first issue is that there may be several ways to *realize* K as a subfield of L. Take $L = \mathbb{R}$, and consider the monic polynomial $p(x) := x^3 - 3x - 1 \in \mathbb{Q}[x]$.

- This is clearly irreducible. (Otherwise, by Gauss's Lemma, it would factor over $\mathbb{Z}$ into a quadratic and linear factor, hence possess an integral root dividing the constant term 1. But $p(1) = -3$ and $p(-1) = 1$, contradiction.)
- So $K := \mathbb{Q}[x]/(p(x))$ is a field. (Let's remind ourselves of how to see this explicitly. For convenience, we may write $K = \mathbb{Q}[\theta]$ where $\theta := \bar{x}$ is the image of x under $\mathbb{Q}[x] \twoheadrightarrow \mathbb{Q}[x]/(p(x))$. Now given any $q(x) \in \mathbb{Q}[x] \setminus (p(x))$, we have $\gcd(p, q) = 1$; so applying the Euclidean algorithm in $\mathbb{Q}[x]$ yields $g, h \in \mathbb{Q}[x]$ with $qg + ph = 1$. So for any $q(\theta) \in K \setminus \{0\}$, we have $g(\theta) = q(\theta)^{-1}$.)
- As an element of $\mathbb{R}[x]$, $p(x)$ splits into distinct linear factors, i.e. has 3 real roots $\theta_1, \theta_2, \theta_3 \in \mathbb{R}$. (Let's be lazy and use Calculus, specifically the intermediate value theorem: we have $p(-2) = -3$, $p(-1) = 1$, $p(1) = -3$, and $p(2) = 1$, which is enough.)

So we get three different ring homomorphisms[2]

$$\begin{aligned} \varphi_i\colon \mathbb{Q}[x] &\to \mathbb{R} \\ x &\mapsto \theta_i \end{aligned}$$

[1] Such a homomorphism is automatically injective (why?). We will usually refer to the homomorphism itself as an **embedding**.

[2] Note that φ_i necessarily is the "identity" on $\mathbb{Q}$, so we don't have to specify that.

which all have kernel $(p(x))$. (Clearly $\ker(\varphi_i) \supseteq (p(x))$ for each i; and $(p(x))$ is a maximal ideal in $\mathbb{Q}[x]$ by irreducibility of p.) By the Fundamental Theorem for ring homomorphisms, these produce three distinct embeddings $\bar{\varphi}_i \colon K = \mathbb{Q}[\theta] \hookrightarrow \mathbb{R}$, sending $\theta \mapsto \theta_i$.

However, the images $\varphi_i(K)$ are in fact equal. This is because, given a root θ of p, $2 - \theta^2$ is another root, and so (using $\theta^3 = 3\theta + 1$) $2 - (2 - \theta^2)^2 = \theta^2 - \theta - 2$ is a third. These are distinct by unique representation of elements of a cubic number field by expressions of the form $a\theta^2 + b\theta + c$. So we find that, for any i, $\mathbb{Q}[\theta_i]$ contains all three $\{\theta_j\}$.

If you like, you can get your hands on the roots as follows: write $\zeta_k := e^{\frac{2\pi\sqrt{-1}}{k}} \in \mathbb{C}$; then $\theta_i = \zeta_{18}^{1+3i} + \overline{\zeta}_{18}^{1+3i} = 2\cos((20 + 60i)^\circ)$ does the job.

I.A.3. EXAMPLE. The second issue, as you may have guessed, is that we may not get so lucky as we did at the end of the last example, and these "realizations" may truly yield distinct subfields of L. Take $L = \mathbb{C}$, and look at $p(x) := x^3 - 2$.

- This is irreducible, by Eisenstein and Gauss.
- Hence $K := \mathbb{Q}[x]/(p(x)) = \mathbb{Q}[\theta]$ is a field.
- In $\mathbb{C}[x]$, we have

$$p(x) = \prod_{i=1}^{3}(x - \theta_i) = (x - \sqrt[3]{2})(x - \zeta_3\sqrt[3]{2})(x - \zeta_3^2\sqrt[3]{2}).$$

Defining φ_i as before, we see that $\varphi_1(K)$ lives inside $\mathbb{R}$, whereas $\varphi_2(K)$ and $\varphi_3(K)$ most certainly do not. In fact, all three are distinct subfields of $\mathbb{C}$.

For most of the remainder of the section, we shall use the notation L/K for field extensions; you can just think of K as a subfield of L.

I.A.4. PROPOSITION. *Given an extension L/K, L is a vector space over K.*

PROOF. Recalling that a K-vector space is the same thing as a K-module (since K is a field), simply define the module structure

by multiplication ($k \cdot \ell := k\ell$) and check the axioms in [**Algebra I**, IV.A.1]. □

I.A.5. DEFINITION. The **degree** of L/K is the vector-space dimension $[L{:}K] := \dim_K(L)$; the extension is called *finite* or *infinite* depending on this degree.

There is a useful visual representation of degrees:

$$\begin{array}{c} L \\ \Big| \\ {\scriptstyle [L:K]} \\ K \end{array}, \qquad \text{e.g.} \qquad \begin{array}{c} \mathbb{C} \\ \Big| \\ {\scriptstyle 2} \\ \mathbb{R} \end{array}, \qquad \begin{array}{c} \mathbb{R} \\ \Big| \\ {\scriptstyle \infty} \\ \mathbb{Q} \end{array},$$

which motivates the

I.A.6. THEOREM (Tower Law). *Given M/L and L/K extensions,*

$$[M{:}K] = [M{:}L][L{:}K]. \tag{I.A.7}$$

PROOF. Say RHS(I.A.7) $= mn < \infty$, and $x_1, \dots, x_m \in M$ [resp. $y_1, \dots, y_n \in L$] is a basis over L [resp. K]. I claim that the $\{x_i y_j\}$ are a basis for M over K (yielding (I.A.7)):

$$\begin{array}{c} M \\ \Big| \\ {\scriptstyle m} \\ L \\ \Big| \\ {\scriptstyle n} \\ K \end{array} \quad {\scriptstyle mn}$$

- They span: given $\mu \in M$, we have $\ell_i \in L$ such that $\mu = \sum_i \ell_i x_i$. Moreover, for each ℓ_i, there exist $k_{ij} \in K$ such that $\ell_i = \sum_j k_{ij} y_j$. Hence $\mu = \sum_{i,j} k_{ij} x_i y_j$.
- They are independent: if $0 = \sum_{i,j} \gamma_{ij} x_i y_j$ ($\gamma_{ij} \in K$), then writing $\delta_i := \sum_j \gamma_{ij} y_j \in L$, we have $0 = \sum_i \delta_i x_i$. Since $\{x_i\}$ is a basis of M/L, all $\delta_i = 0$; and then since $\{y_j\}$ is a basis of L/K, $\gamma_{ij} = 0$.

Conversely if LHS(I.A.7) $= \ell < \infty$, let $z_1, \dots, z_\ell \in M$ be a basis over K. Since these span M as a vector space over L, $[M{:}L] < \infty$. Moreover, $[L{:}K] < \infty$ since L/K is a vector subspace of the finite-dimensional vector space M/K.[3] Hence RHS(I.A.7) $< \infty$ and we get (I.A.7) as before. □

[3] Let A_0 be a maximal linearly independent subset of L/K, which exists (and is finite) since $[M{:}K] < \infty$. Clearly this must span L.

I.A.8. REMARK. Given L_1/L_0, L_2/L_1, ..., L_n/L_{n-1}, inductively applying I.A.6 yields

$$[L_n{:}L_0] = \prod_{i=1}^{n} [L_i{:}L_{i-1}].$$

This all seems rather stupid, but it's actually powerful when used in the right way. For instance, ask yourself: if $[M{:}K]$ is a prime number, what fields are intermediate between M and K?

I.A.9. COROLLARY. *If M/K is an extension, and $L \subset M$ is a subfield containing K, then $[L{:}K] \big| [M{:}K]$.*

We want to study intermediate extensions generated by elements. Suppose L/K is an extension, and $\mathcal{S} \subset L$ is a subset.

I.A.10. DEFINITION. The extension $K(\mathcal{S})$ of K *generated by* $\mathcal{S}$ is the intersection of all subfields of L containing $K \cup \mathcal{S}$. (We write $K(\alpha_1, \ldots, \alpha_m)$ for $K(\{\alpha_1, \ldots, \alpha_m\})$.)

An immediate consequence of the definition is that for a pair of sets $\mathcal{S}, \mathcal{T}$ we have $K(\mathcal{S})(\mathcal{T}) = K(\mathcal{S} \cup \mathcal{T})$, which wil be written $K(\mathcal{S}, \mathcal{T})$. A special case is when K_1 and K_2 are subfields of L containing K; then $K(K_1, K_2)$ is the smallest subfield containing both K_1 and K_2, called their **compositum**.

A more concrete description of these extensions is given by the

I.A.11. PROPOSITION. *Set $\tilde{\mathcal{S}} := \{\prod_{i=1}^{k} s_i \mid k \in \mathbb{Z}_{>0},\ s_i \in \mathcal{S}\} \cup \{1\}$, and $V := K\langle \tilde{\mathcal{S}} \rangle$ the K-linear span. Then*

$$K(\mathcal{S}) = \{vu^{-1} \mid v \in V,\ u \in V \setminus \{0\}\}.$$

PROOF. The inclusion "$\subseteq$" is clear because the RHS is a subfield of L (i.e. is closed under addition etc.). The reverse inclusion is clear since any field containing $K \cup \mathcal{S}$ must contain these elements. □

I.A.12. DEFINITION. An extension L/K is **simple** if there exists $u \in L$ such that $L = K(u)$, in which case u is called a **primitive element** for the extension.

I.A.13. EXAMPLES. (i) $\mathbb{C}/\mathbb{R}$ and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ are simple.
(ii) $\mathbb{R}/\mathbb{Q}$ is not simple: given any $r \in \mathbb{R}$, I.A.11 gives

$$\mathbb{Q}(r) = \left\{ \tfrac{p(r)}{q(r)} \mid p, q \in \mathbb{Q}[r];\, q \neq 0 \right\},$$

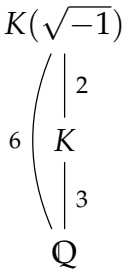
which is clearly a countable set, whereas $\mathbb{R}$ is uncountable.
(iii) If $[L{:}K]$ is prime, then L/K is simple. (Why?)

I.A.14. EXAMPLE. Let $K = \mathbb{Q}[x]/(p(x))$, with $p(x) = x^3 - 3x - 1$ as in I.A.2, and take $u \in K^*$. Let's consider the simple extension

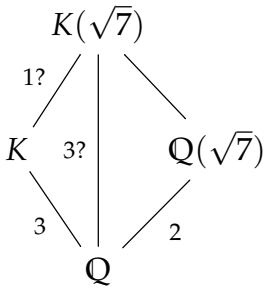
$$L := K(\sqrt{-u}) := \begin{cases} K[y]/(y^2+u), & \text{if } y^2+u \text{ is irreducible over } K \\ K, & \text{otherwise.} \end{cases}$$

The question is how to know which case we are in on the RHS; if $L \supsetneq K$, we say that the extension is **proper**.

We can use $\varphi_i \colon K \hookrightarrow \mathbb{R}$ to think of L/K as $\varphi_i(K)(\sqrt{-\varphi_i(u)})/\varphi_i(K)$. In this way, we see that *if any $\varphi_i(u) > 0$, then the extension is proper.* Indeed, if it is *not* proper, then we have a $k \in K$ such that $k^2 = -u$, hence $\varphi_i(k)^2 = -\varphi_i(u)$, a contradiction. So for example, since $\varphi_i(1) = 1 > 0$ (for any i), we get the tower shown at right.



What about the converse of the italicized statement? That is, if every $\varphi_i(u) < 0$, then is the extension trivial ($L = K$)? Consider $u = -7$, for instance, and the extension diagram shown. If $K(\sqrt{7}) = K$, we get the degrees shown with a "?", which contradict the Tower Law since $2 \nmid 3$. So we must have $[K(\sqrt{7}){:}K] = 2$, and the converse fails.



So the Tower Law is pretty effective: it shows that if a rational number isn't a square in $\mathbb{Q}$, it isn't a square in K either, with no work.

Let L/K be an extension, $u \in L$, and consider the simple extension $K(u)/K$. We have as usual the evaulation map

$$\mathrm{ev}_u \colon K[x] \twoheadrightarrow K[u]$$

sending $x \mapsto u$, with kernel $(f(x))$ (since $K[x]$ is a PID). Since the image is a domain, f must be irreducible. There are then two cases:

Case 1: $\ker \neq \{0\} \implies K[u]$ is a field ($=K(u)$), with $f = m_u$ (normalized to be monic) the minimal polynomial of u.

Case 2: $\ker = \{0\} \implies \mathrm{ev}_u$ is an isomorphism $\implies \mathrm{ev}_u$ extends uniquely to an isomorphism $K(x) \xrightarrow{\cong} K(u)$ of fraction fields.

I.A.15. DEFINITION. In Case 1, $u \in L$ is **algebraic** over K.
In Case 2, $u \in L$ is **transcendental** over K.

I.A.16. THEOREM. *Given $u \in L$, L/K. Then*
(i) *u is algebraic* $\iff [K(u):K] < \infty$.
(ii) *In this case,* $[K(u):K] = \deg(m_u)$.

PROOF. If u is algebraic, then $K(u) = K[u] \cong K[x]/(m_u(x))$, a basis over K for which is $1, x, \ldots, x^{d-1}$ (where $d = \deg(m_u)$). Conversely, if $n := [K(u):K] < \infty$, we can't be in Case 2, since already $\dim_K(K[x]) = \infty$ there (and $K(u) = K(x)$ is still bigger). □

I.A.17. COROLLARY. *Given L/K,*

$$L_{alg/K} := \{\alpha \in L \mid \alpha \text{ algebraic over } K\}$$

is a subfield.

PROOF. Let $\alpha, \beta \in L_{\mathrm{alg}/K}$. Then β is algebraic over $K(\alpha)$, so

$$[K(\alpha,\beta):K] = [K(\alpha)(\beta):K(\alpha)][K(\alpha):K] < \infty.$$

Since $K(\alpha\beta)$ and $K(\alpha+\beta)$ are sub-K-vector spaces of $K(\alpha,\beta)$, they have finite dimension/degree over K. By I.A.16(i), we therefore have $\alpha\beta, \alpha+\beta \in L_{\mathrm{alg}/K}$. Finally, if $\alpha \neq 0$, set $\mu(x) := x^n m_\alpha(\frac{1}{x})$, with $n := \deg(m_\alpha)$; then we have $\mu(\frac{1}{\alpha}) = \alpha^{-n} \cancelto{0}{m_\alpha(\alpha)} = 0 \implies \frac{1}{\alpha} \in L_{\mathrm{alg}/K}$. □

I.A.18. EXAMPLE. Consider $\mathbb{C}/\mathbb{Q}$. Define $\bar{\mathbb{Q}} := \mathbb{C}_{\mathrm{alg}/\mathbb{Q}}$ in the above sense. This is the field of **algebraic numbers**. (Obviously it contains the ring of algebraic integers $\bar{\mathbb{Z}}$.)

I.A.19. DEFINITION. An **algebraic extension** L/K is one with $L = L_{\mathrm{alg}/K}$. That is, every element of L is algebraic over K.

Finite extensions are algebraic. (Why? If L/K is finite, and $\alpha \in L$, then $[K(\alpha):K] \leq [L:K] < \infty$.) Are algebraic extensions finite? Certainly not in general, as $\bar{\mathbb{Q}}/\mathbb{Q}$ demonstrates. But we do have the

I.A.20. PROPOSITION. *The following are equivalent:*
(a) $[L:K] < \infty$.
(b) *L/K is algebraic and L is finitely generated over K (in the field sense).*
(c) *$L = K(\alpha_1, \ldots, \alpha_n)$, with each α_i algebraic over K.*

PROOF. (a) $\implies$ (b): L/K is algebraic since $[K(\alpha):K] \leq [L:K] < \infty$ for any $\alpha \in L$. If $a_1, \ldots, a_n$ is a basis for L/K then $L = K(a_1, \ldots, a_n)$.
(b) $\implies$ (c): obvious.
(c) $\implies$ (a): apply the Tower Law, together with

$$[K(\alpha_1, \ldots, \alpha_{k-1})(\alpha_k):K(\alpha_1, \ldots, \alpha_{k-1})] \leq [K(\alpha_k):K] < \infty$$

for each k). □

I.A.21. COROLLARY. *If $\mathcal{S} \subset L$ is a (possibly infinite) set of elements algebraic over K, then $K(\mathcal{S})/K$ is an algebraic extension (possibly infinite).*

PROOF. $\beta \in K(\mathcal{S}) \implies$ there exist $\alpha_1, \ldots, \alpha_n \in \mathcal{S}$ such that $\beta \in K(\alpha_1, \ldots, \alpha_n) \implies [K(\beta):K] < \infty$. □

I.A.22. COROLLARY. *If M/L and L/K are both algebraic extensions, then M/K is algebraic.*

PROOF. We want to show that each $\alpha \in M$ is algebraic over K. Consider its minimal polynomial $m_\alpha(x) = \sum_{j=0}^{n} \ell_j x^j$ with respect to L. This exhibits α as algebraic over $K(\ell_0, \ldots, \ell_n)$, which by I.A.20 is finite over K. Now apply the Tower Law. □

Automorphisms of field extensions are one of the key concepts in Galois theory. We finish with the following

I.A.23. PROPOSITION. *Suppose L/K is algebraic and $\tau\colon L \to L$ is a field homomorphism fixing K pointwise: $\tau(k) = k$ $(\forall k \in K)$. Then $\tau(L) = L$; that is, τ is an automorphism.*

PROOF. Given $\alpha \in L$ with minimal polynomial m_α over K, let R be the set of roots of m_α in L. We know only that $\alpha \in R$ and $|R| \leq \deg(m_\alpha)$.

If $\beta \in R$, then (since coefficients of m_α are in K hence fixed by τ)

$$m_\alpha(\tau(\beta)) = \tau(m_\alpha(\beta)) = \tau(0) = 0$$

and thus $\tau(R) \subset R$. Since τ is injective (like any field homomorphism), and R is finite, $\tau(R) = R$.

We conclude that $\alpha \in \tau(L)$; and since α was arbitrary, τ is surjective. □